大專院校
外部資安評級情資服務
情資驅動的資安防禦趨勢
簡報

創穩資云

陳勇君 執行長/博士

Sunrise@CyberWin.com.tw

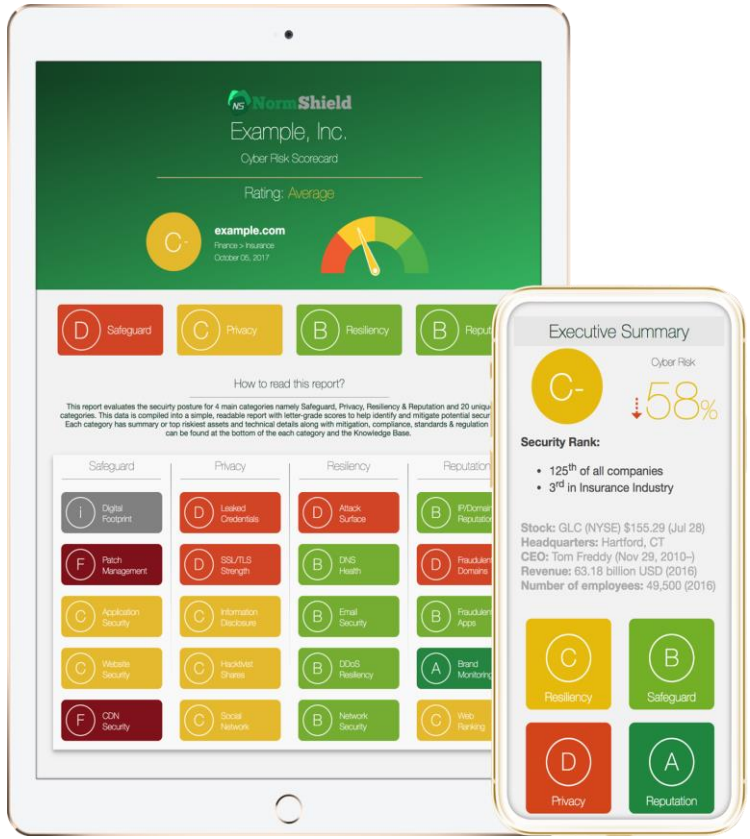
CISSP

ISO 27001, 27701 LA

CyberWin
創穩資云

內容綱要

- 大專院校資安防護的挑戰
- 何謂【外部資安評級情資服務】?
  - 看不到 + 不知道 = 最令人害怕的潛在風險
- Black Kite 服務介紹
- 為何需要【外部資安評級情資服務】?
- Q & A



大專院校資安防護的挑戰 – 1/2

如何衡量自己學校的資安水平?

- 學校資安做得好不好？【誰】的角度最清楚？

弱掃、滲透、黑白箱結果這麼多，如何修補？

- 【外部可看到】或者【駭客已知道】的弱點，可當作修補【輕重緩急】的優先順序！

資安預算該如何運用/投資？

- 如能瞭解學校各種不同資安構面的資安水平，即可透過【資安木桶理論】來找出【最短木板】，進行【最佳成本效益】投資。

大專院校資安防護的挑戰 – 2/2

如何在【校長/董事會】呈現資安的重要性？

- 怎樣的資安態勢呈現，可以讓【校長/董事會】體認資安投資的重要性！

學校資安要好，可能不是僅要【核心系統】做好即可？

- 學校內各系所、學生社團等所有對外服務 等等都是學校資安的【同船人/生命共同體】！

學校投保【資安險】的趨勢！

- 問題，誰來替學校出【資安/健康檢查】報告？

何謂【外部資安評級情資服務】?

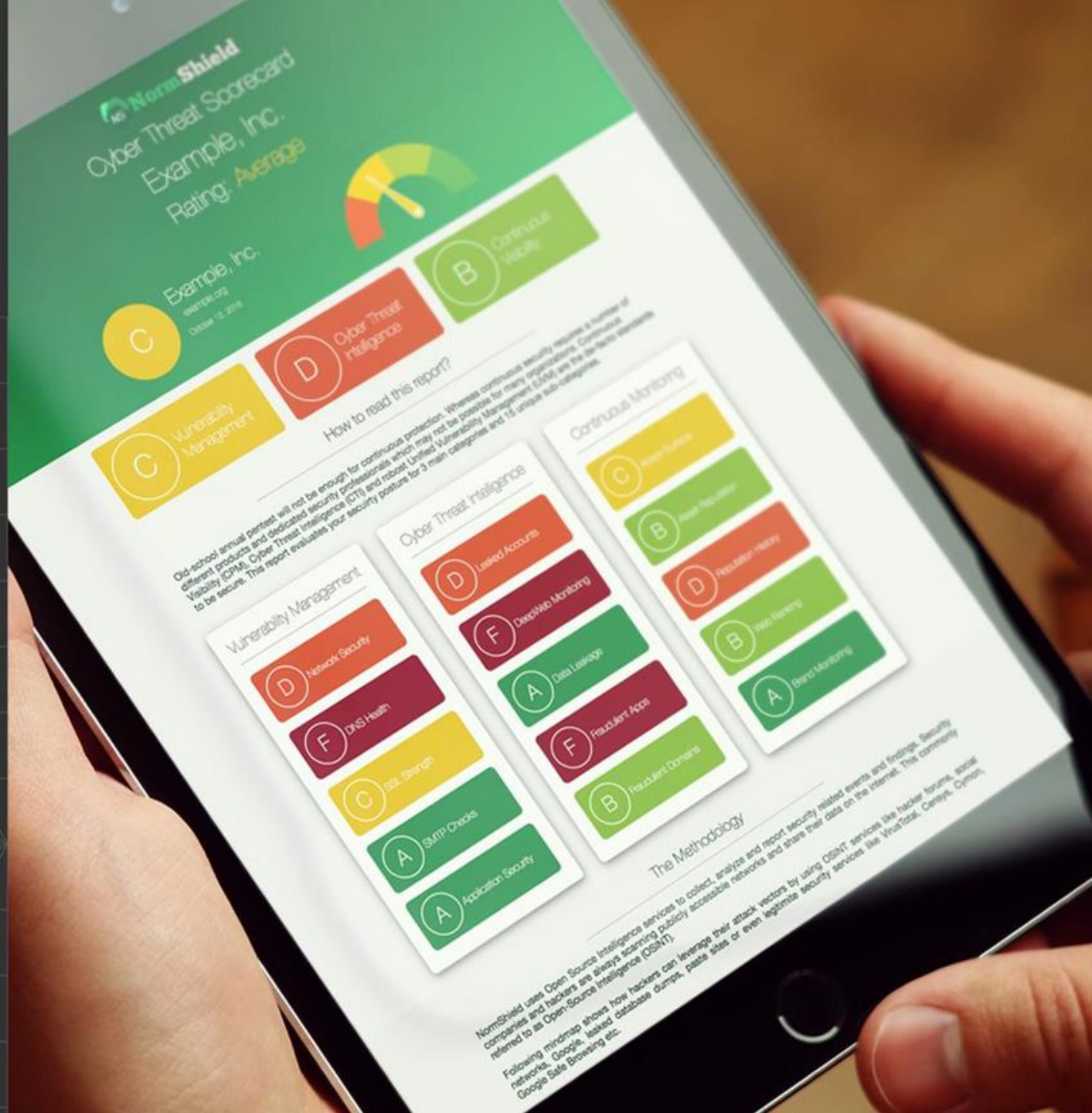
What ?

CyberWin
創穩資云

BLACK KITE®
FORMERLY NORMSHIELD

Cyber Risk Monitoring

Trusted Security Rating Services
【外部資安評級情資服務】



看不到 + 不知道 = 最令人害怕的潛在風險

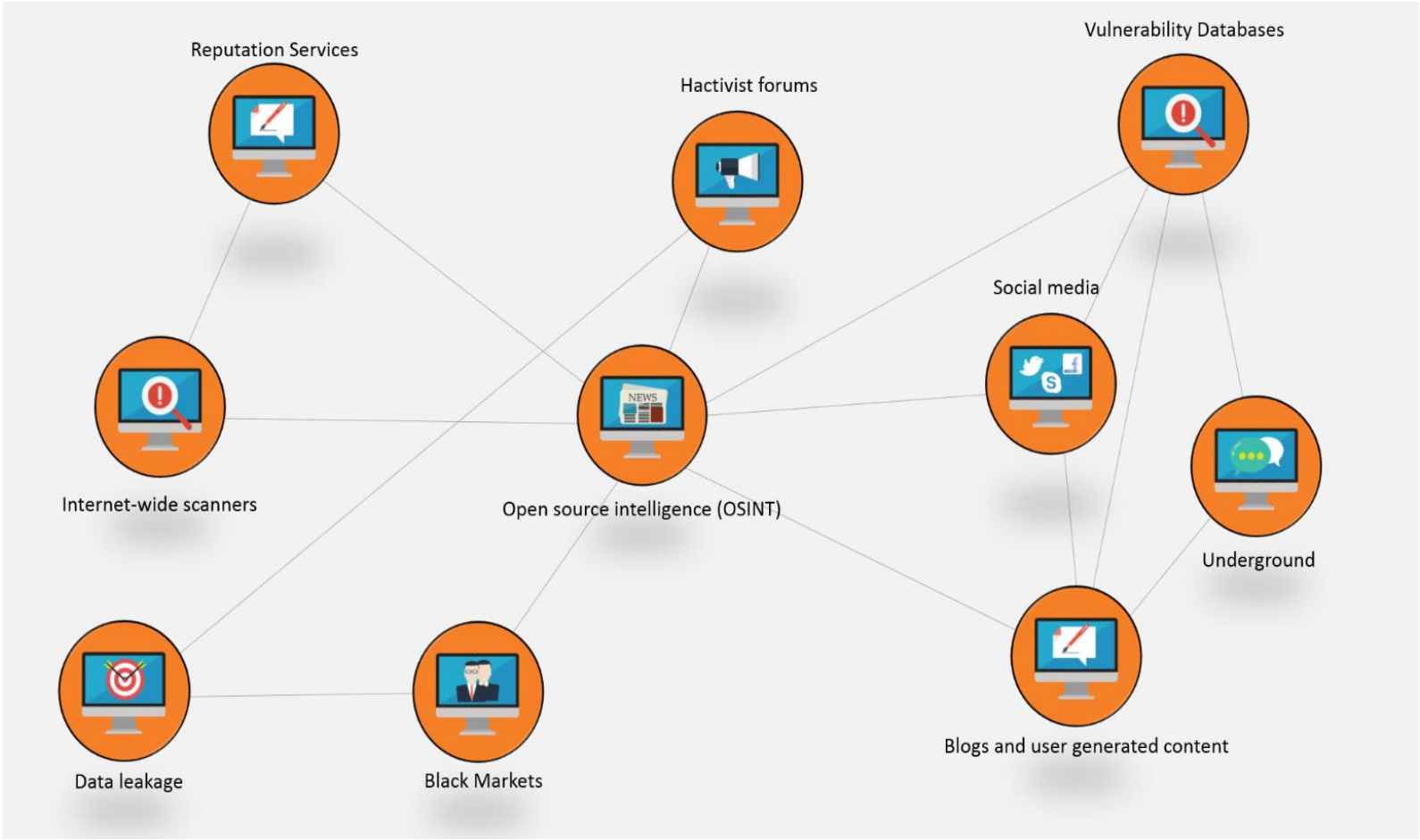
駭客比我們更清楚我們的弱點與漏洞問題？

- 網際空間【隨時隨地】有人在弱掃我們、探索我們、攻擊我們、竊取我們，而且【私密分享】與【任意公布】這些資安風險情資!
- 學校對外網路服務因為競爭也時時因應【調整創新】，如有【不慎疏忽】，便讓駭客持續的攻擊弱掃探索而【被發現新的問題】!
- 然而每間大專院校真的知道網駭空間(Cyber Space Security)中自己所有【數位足跡/漏洞問題】的分布狀況?
  - 真是【瞭然於胸】清清楚楚？還是【層層問號】不知不覺?

何謂【外部資安評級情資服務】?

- (a)【沒有】侵入式弱掃
- 也【沒有】進行滲透測試
- 而是完整收集網際網路上面(包含暗網，駭客論壇，地下弱掃網站、情蒐網站、OSINT、Censys、Shodan、Zoomeye)的大數據分析。

- (b) 以【外部與駭客】角度
- 檢視企業機關的【全球數位足跡(Digital Footprint)】
- 運用【4 個】資安構面，【20 個】資安領域類別來分析 貴企業機關 的資安等級
- 也包含貴企業機關在【同業水平】的資安評價比較



【外部資安評級情資服務】方法論

某學術單位的外部曝露之【數位足跡】資訊資產

2,175 個
外部服務資訊資產

Digital Footprint of AAA 單位 (2175 assets)

Passive threat scanning collects information from the internet (hacker sites, security information sharing sites, internet wide-scanners, reputation services, search engines, etc.). Digital Footprint is determined by using open ports, services and application banners. This information is gathered from several sources like Black Kite, Censys, VirusTotal, Robtext, NetCraft, etc.

Domains 12 | IP 200 | Subdomains 796 | Dns Records 60 | Services 379 | Social Media 2 | Asn 6 | E-Mails ! | Geo Map | Company Information

Http 85 | Https 85 | Ftp 11 | Smtp/Mail 3 | Telnet/Ssh 15 | Dns 0 | Others 180

外部服務/資訊資產
明細清單：主要 Domain x 12 個
IP x 200 個
Subdomain x 796 個
Service x 379 個

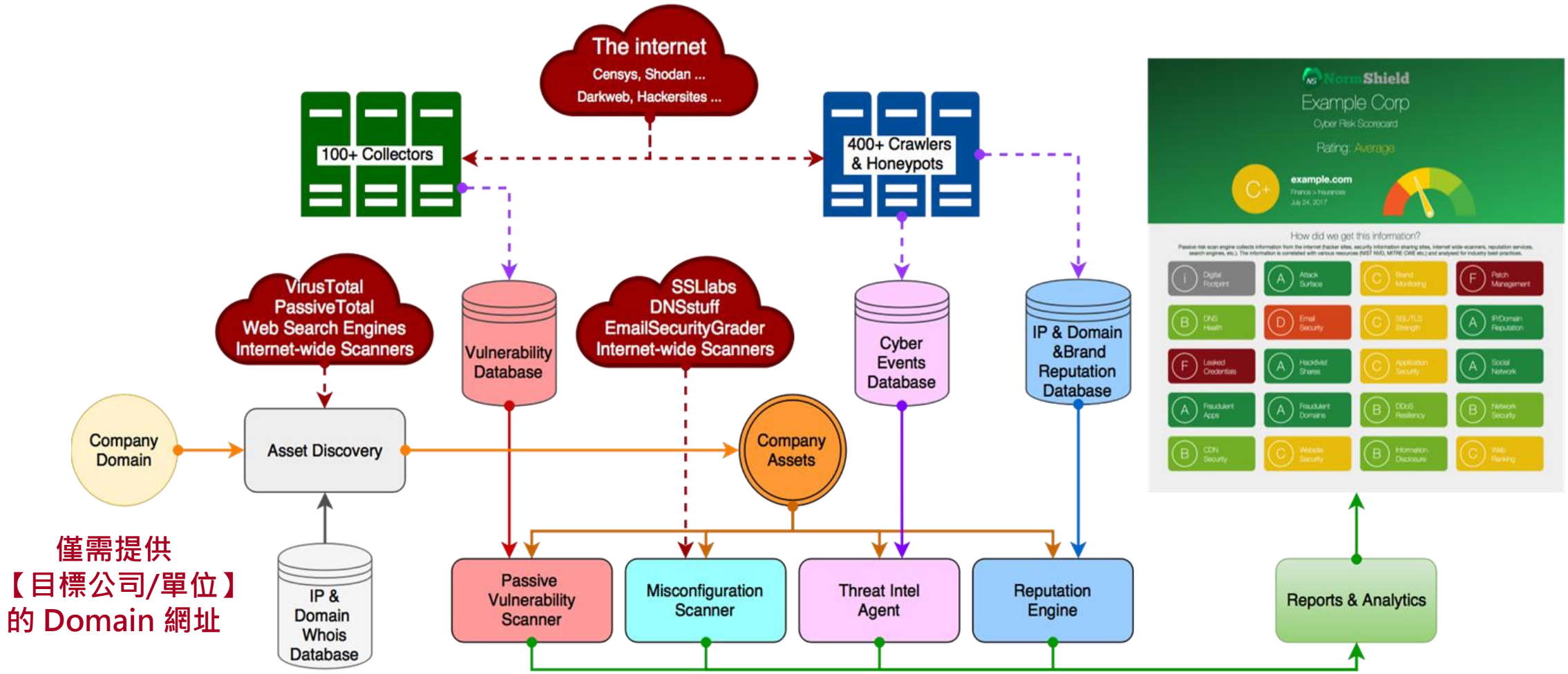
各種外部服務
明細清單：Http/Https x 85/85 個
FTP x 11 個
Email x 3 個
Telnet/SSH x 15 個

BLACK KITE
FORMERLY NORMSHIELD

Black Kite
外部資安評級情資服務
功能介紹

CyberWin
創穩資云

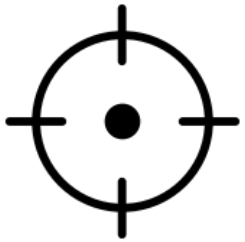
BlackKite 資安風險評級服務之運作架構



僅需提供
【目標公司/單位】
的 Domain 網址

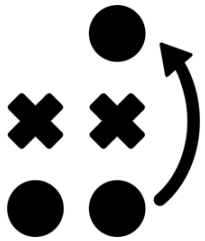
【非侵入性】的被動接觸分析 & 【主動性】的廣泛蒐集【針對性】資安情資

BlackKite【評價計分】方法論 – 公正公開



Establish Assessment Scope

Digital Footprint

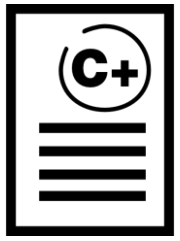


Identify Candidate TTPs

CAPEC
CWE
CVE

Eliminate Implausible TTPs

False Positive Elimination



Apply Scoring Model

CAPEC
CWE
Severity
CVSS / CWSS

Construct the Threat Matrix

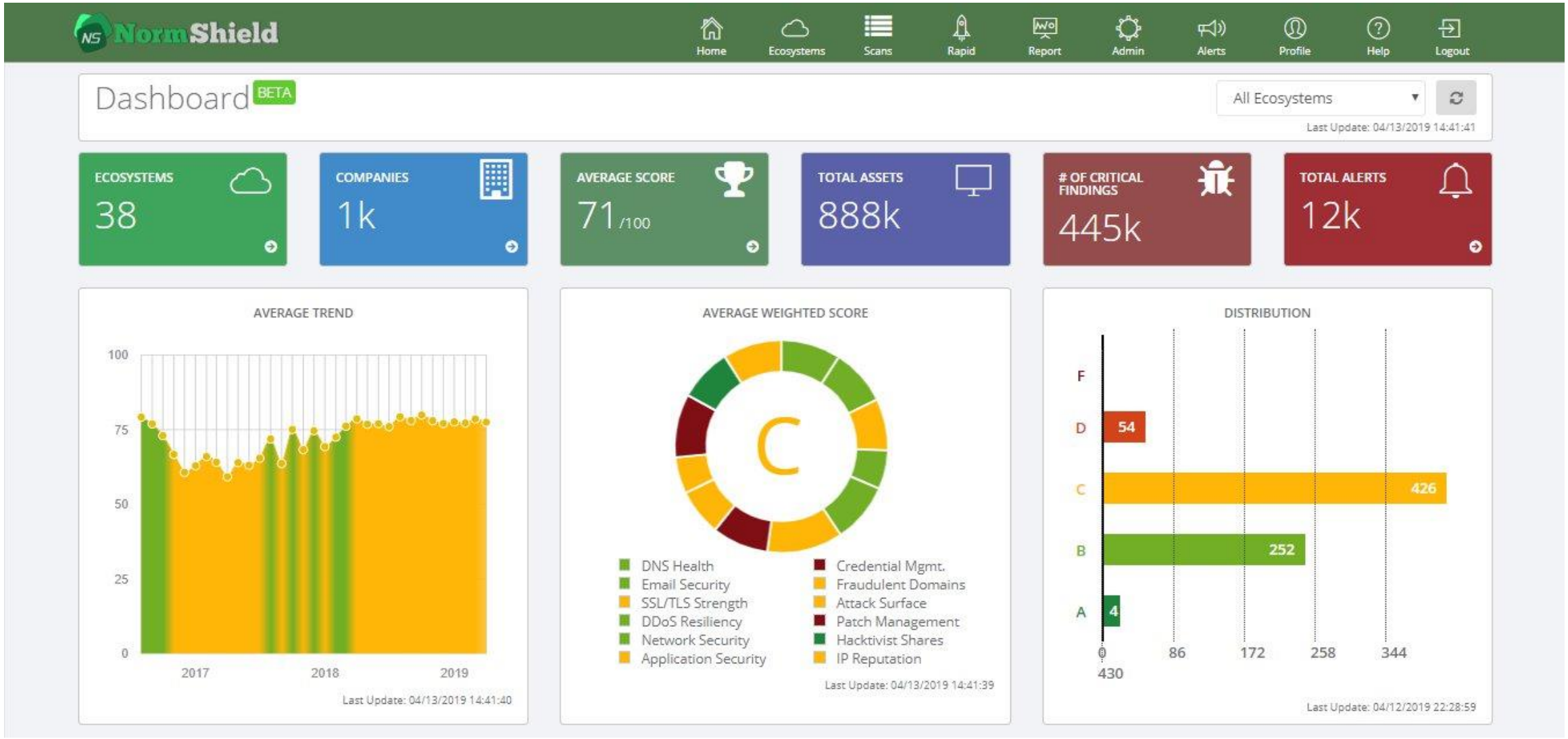
APPSEC-001
APPSEC-002
…
DNSSEC-001

MITRE

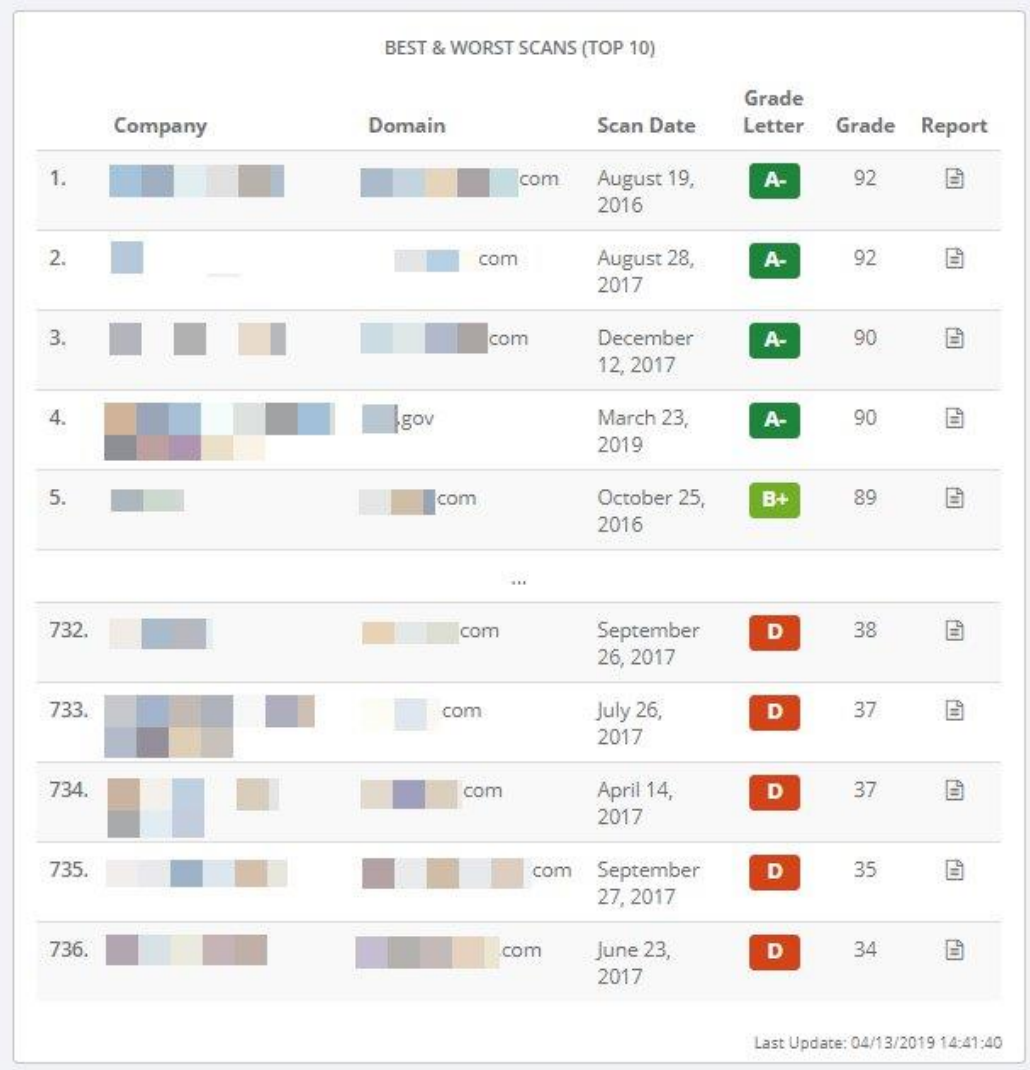
Cyber Threat Susceptibility Assessment (CTSA)

Definition: Cyber Threat Susceptibility Assessment (TSA) is a methodology for evaluating the susceptibility of a system to cyber-attack. TSA quantitatively assesses a system's [in]ability to resist cyber-attack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs) associated with the Advanced Persistent Threat (APT). *[MITRE]*

豐富明瞭的【數位儀表板】


NormShield
Home
Ecosystems
Scans
Rapid
Report
Admin
Alerts
Profile
Help
Logout
Dashboard BETA
All Ecosystems
Last Update: 04/13/2019 14:41:41
ECOSYSTEMS
38
COMPANIES
1k
AVERAGE SCORE
71 /100
TOTAL ASSETS
888k
OF CRITICAL FINDINGS
445k
TOTAL ALERTS
12k
AVERAGE TREND
100
75
50
25
0
2017
2018
2019
Last Update: 04/13/2019 14:41:40
AVERAGE WEIGHTED SCORE
C
DNS Health
Email Security
SSL/TLS Strength
DDoS Resiliency
Network Security
Application Security
Credential Mgmt.
Fraudulent Domains
Attack Surface
Patch Management
Hacktivist Shares
IP Reputation
Last Update: 04/13/2019 14:41:39
DISTRIBUTION
F
D
54
C
426
B
252
A
4
0
86
172
258
344
430
Last Update: 04/12/2019 22:28:59

Top N 資安評級 & Top N 資安風險 for 數位足跡



BEST & WORST SCANS (TOP 10)

	Company	Domain	Scan Date	Grade Letter	Grade	Report
1.		com	August 19, 2016	A-	92	
2.		com	August 28, 2017	A-	92	
3.		com	December 12, 2017	A-	90	
4.		.gov	March 23, 2019	A-	90	
5.		com	October 25, 2016	B+	89	
...						
732.		com	September 26, 2017	D	38	
733.		com	July 26, 2017	D	37	
734.		com	April 14, 2017	D	37	
735.		com	September 27, 2017	D	35	
736.		com	June 23, 2017	D	34	

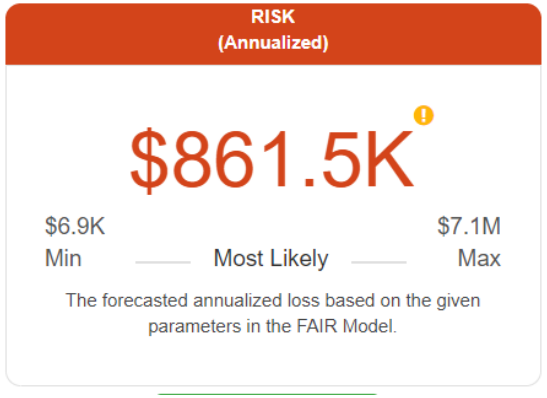
Last Update: 04/13/2019 14:41:40

MOST CRITICAL ISSUES (TOP 10)

	Asset	Risk	Risk Score	Report
1.		CVE-2017-7895 - cpe:/o:linux:linux_kernel:4.10.13	10	
2.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
3.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
4.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
5.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
6.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
7.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
8.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
9.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	
10.		CVE-2016-6137 - cpe:/a:sap:trex:7.10:revision_63	10	

Last Update: 04/13/2019 14:41:40

BlackKite 資安評級計分【三大】指標



資安【技術問題】指標

- 運用 MITRE 公認公開之資安評分標準
- 提供企業機關資安主管快速【資安評級(字母表示法)】
- 讓資安技術主管可以【往下詳探】每個資安領域的安全議題。

資安【事故財損】指標

- FAIR 是目前唯一公開公正的【資安衝擊財損量化模式】的國際標準。
- 因此，NS 使用 FAIR Model 來計算【當單一資安事故發生時，對特定企業機關可能的財物損失衝擊影響】。

資安【合規】指標

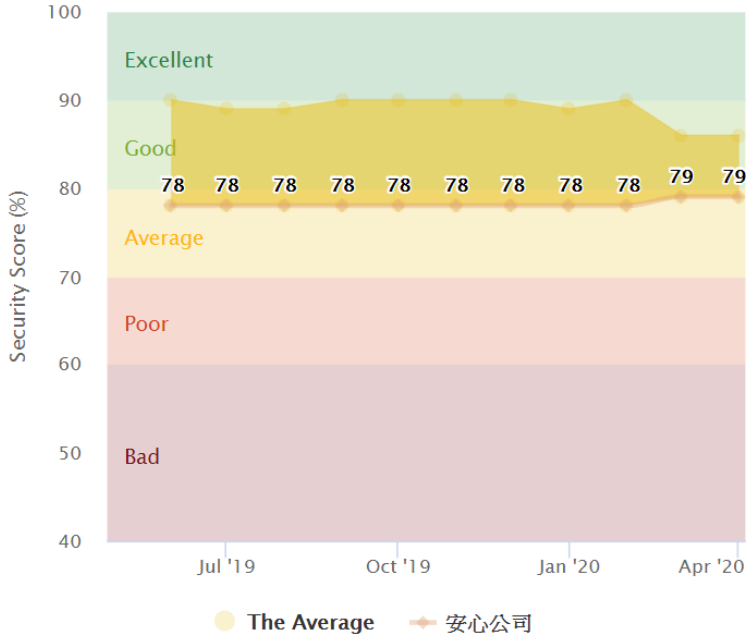
- 根據【網駭空間發現】，關聯分析相對資安標準與法規之控制項目，判別該控制項目可能的符合程度。
- 包含：ISO 27001、PCI-DSS、GDPR、HIPAA、NIST 800-53 等等。

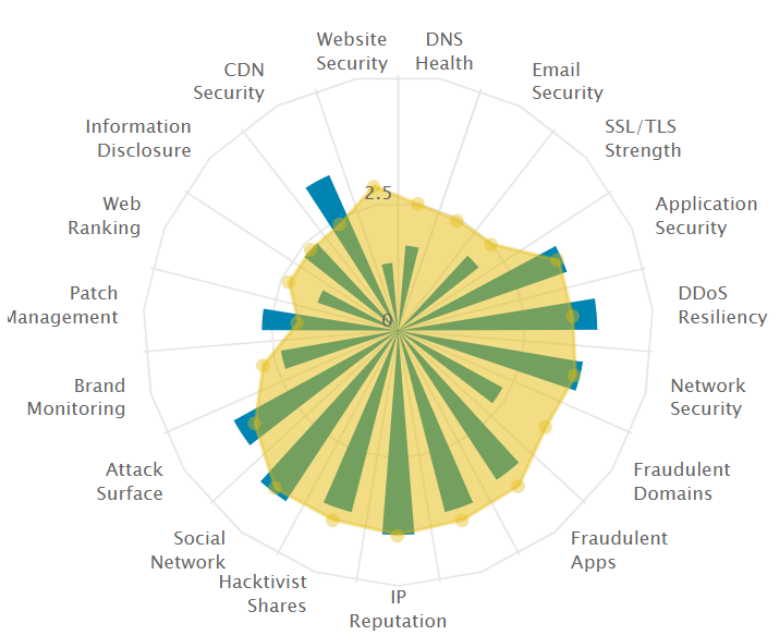
MITRE

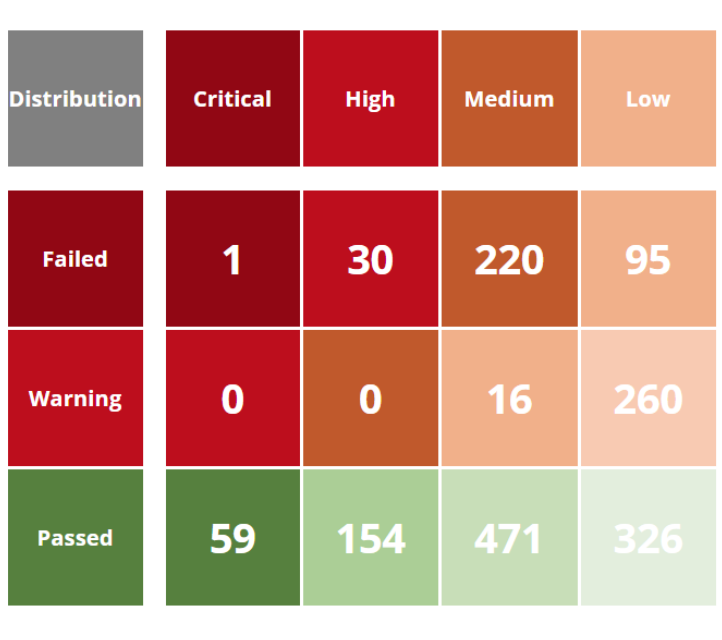
FAIR INSTITUTE

SFG SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

資安評級趨勢變化/同業比較/領域優劣/熱點發現







資安變化/同業比較

【紫色曲線】代表【自己機關】
【黃色區域】代表【同級機關】

每個資安【領域】優劣分析

【藍色條棒】代表【自己機關】
【黃色區域】代表【同級機關】

資安問題【熱點】快搜

主要觀察重點：Failed 的
Critial & High

【20 個】資安領域類別 &【500+】檢查控制項目

【20 個】資安領域類別 &【500+】檢查控制項目

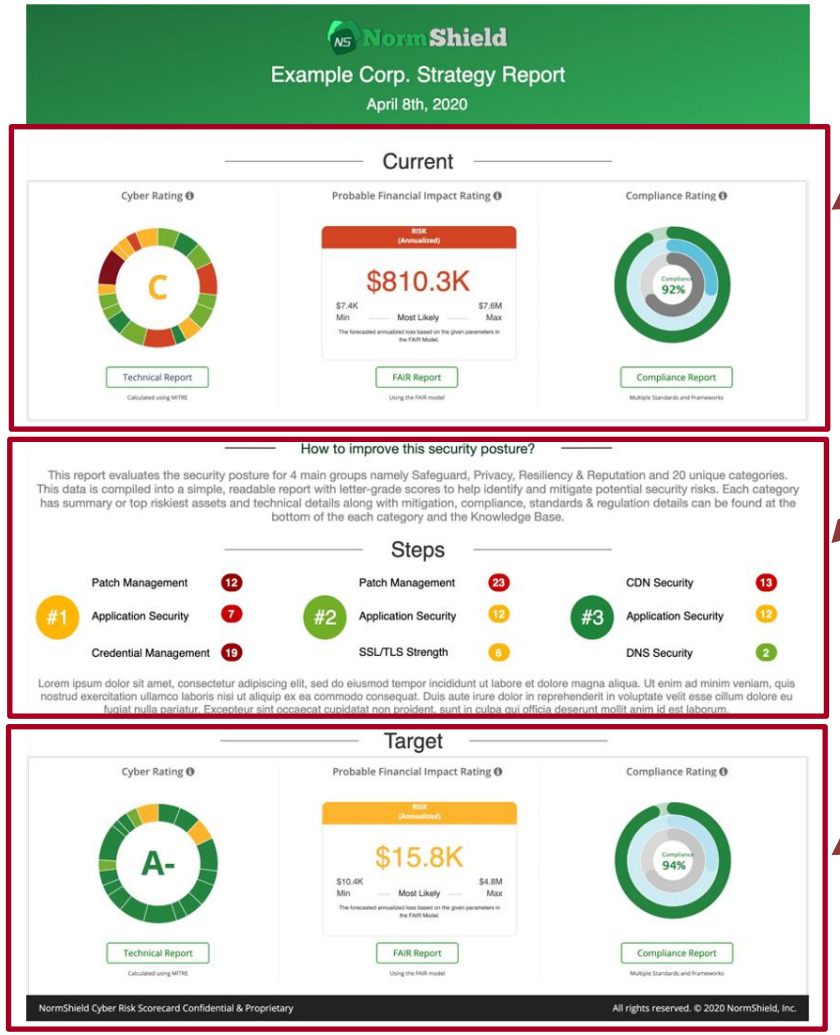
皆可『Drill-Down』到詳細說明

學術【同業/供應鏈】之資安水平快速檢視比較

	甲	乙	丙	丁	戊	己	庚	辛
Overall	C+	B+	B	B	B-	B-	C+	C+
Safeguard	C	A	B	B	B	D	C	D
Privacy	B	A	B	B	B	B	B	B
Resiliency	C	B	B	B	C	B	B	B
Reputation	B	A	A	B	A	A	B	B

資安水平快速檢視比較【BenchMark】

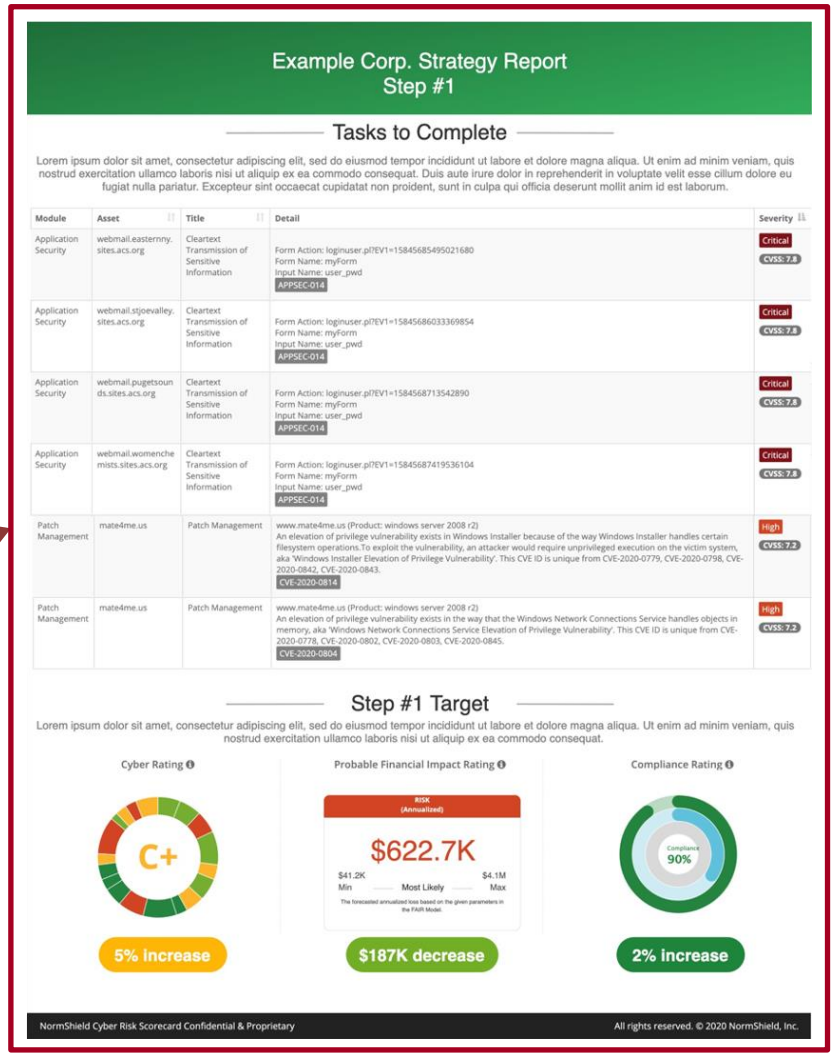
評級分數【改善成長】計劃策略



目前
資安評級

建議
改善成長
計劃
Step
1~3

未來期待
資安評級



BlackKite 的資安技術指標之字母定義

	Grade	Percentage over 100
Excellent	A+	97 <= x < 100
	A	93 <= x < 97
	A-	90 <= x < 93
Good	B+	87 <= x < 90
	B	83 <= x < 87
	B-	80 <= x < 83
Average	C+	77 <= x < 80
	C	73 <= x < 77
	C-	70 <= x < 73
Poor	D+	67 <= x < 70
	D	63 <= x < 67
	D-	60 <= x < 63
Bad	F	0 <= x < 60
	i	Information
	n/a	Not Available

20 個資安構面的分數【權重比例】說明

Category Name	Weight (Total 100)
Digital Footprint	0/100
DNS Health	6/100
Email Security	6/100
SSL/TLS Strength	6/100
Application Security	9/100
DDoS Resiliency	4/100
Network Security	6/100
Fraudulent Domains	5/100
Fraudulent Apps	3/100
Credential Mgmt.	9/100
IP Reputation	7/100
Hacktivist Shares	5/100
Social Network	3/100
Attack Surface	4/100
Brand Monitoring	3/100
Patch Management	10/100
Web Ranking	2/100
Information Disclosure	3/100
CDN Security	3/100
Website Security	6/100

外部資安評級情資服務 vs 弱掃/滲透/黑白箱檢測

	檢視範圍	檢視廣度	檢視頻率	檢視角度
弱掃/滲透/黑白箱	● 學校【核心系統】 ● 範圍【較小】	• 範圍內【特定】服務，較小 • (80/443)	• 週期性 • 每月/每季/每年 • 頻率【低】 • 空窗期長	• 內部角度 • 同仁角度 • 廠商角度 • 易有盲點
外部資安評級情資服務	● 學校所有對外系統(資訊單位、行政單位、系所、學生社團 ...) ● 範圍【較大】	• 範圍內【所有對外服務】較廣 • DNS/Email/Web/FTP/...	• 每天 • 頻率【高】 • 幾乎沒有空窗期	• 外部角度 • 駭客角度 • 盲點甚低

為何需要
【外部資安評級情資服務】？

Why

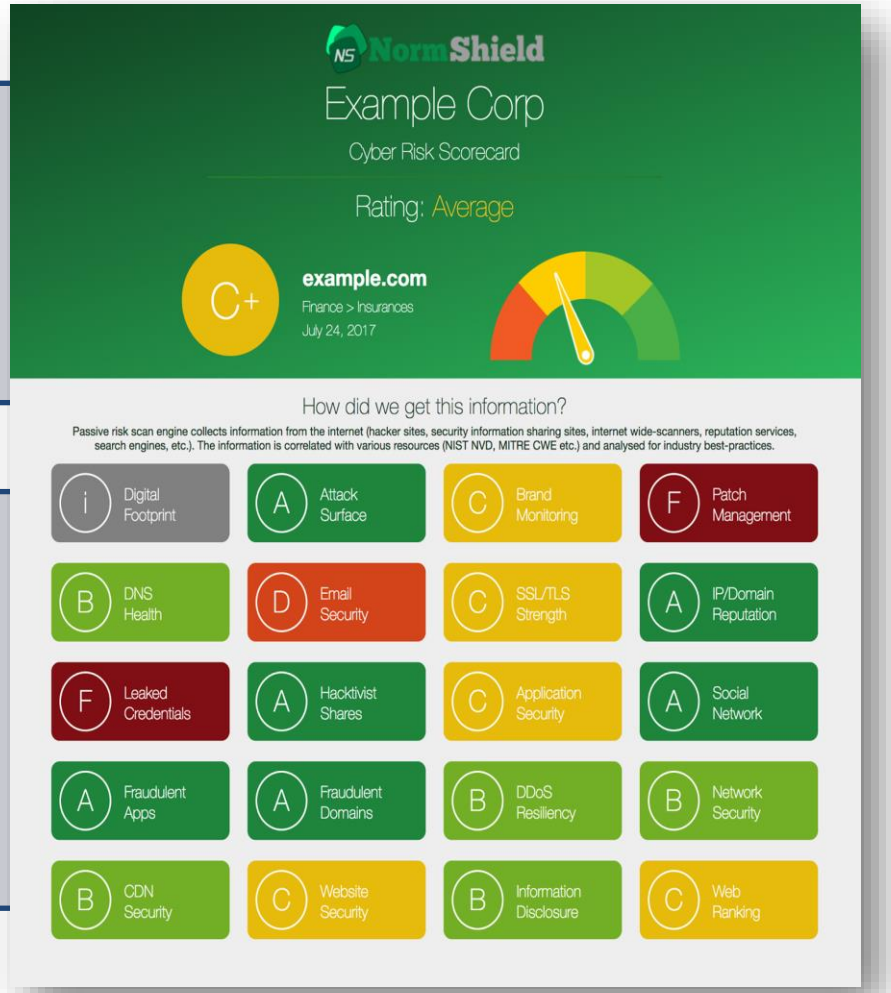
為何需要【外部資安評級情資服務】？1/3

知己

- 如何衡量公司目前【資安成效】？
  - 是自我【感覺良好】？還是【身陷風險而不自知】？

知彼

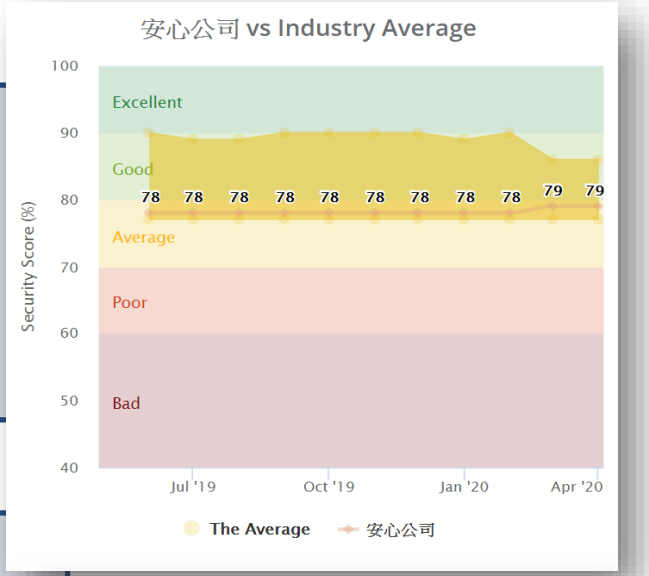
- 如何了解【外部駭客】對【單位資安水平】的看法?
  - 是【固若金湯】？還是【暗潮洶湧】？
  - 是【無懈可擊】？還是【漏洞百出】？



為何需要【外部資安評級情資服務】？2/3

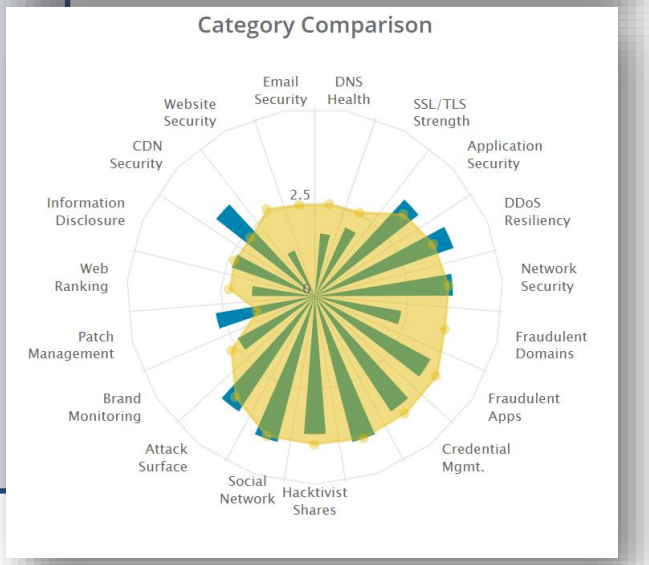
同業比較

- 如何了解公司與同業之間資安水平的比較?
  - 是【名列前茅】？還是【水平之下】？



資安投資

- 如何了解資安投資的正確方向？
  - 是【人云亦云】？還是【資源放刀口】？
- 資安水桶理論：
  - 加長【最長木板】，還是【最短木板】？



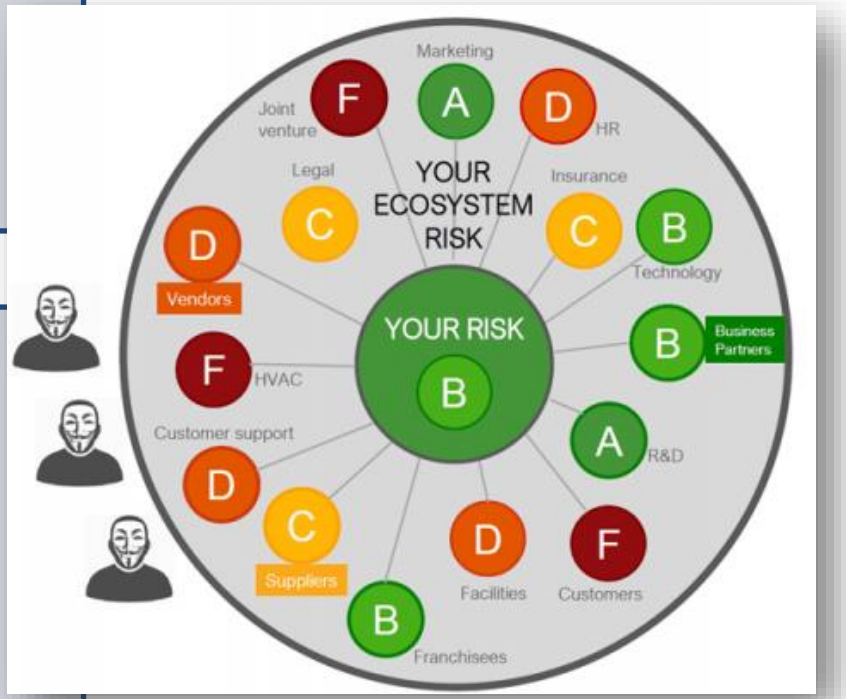
為何需要【外部資安評級情資服務】？3/3

關係企業/系所/社團

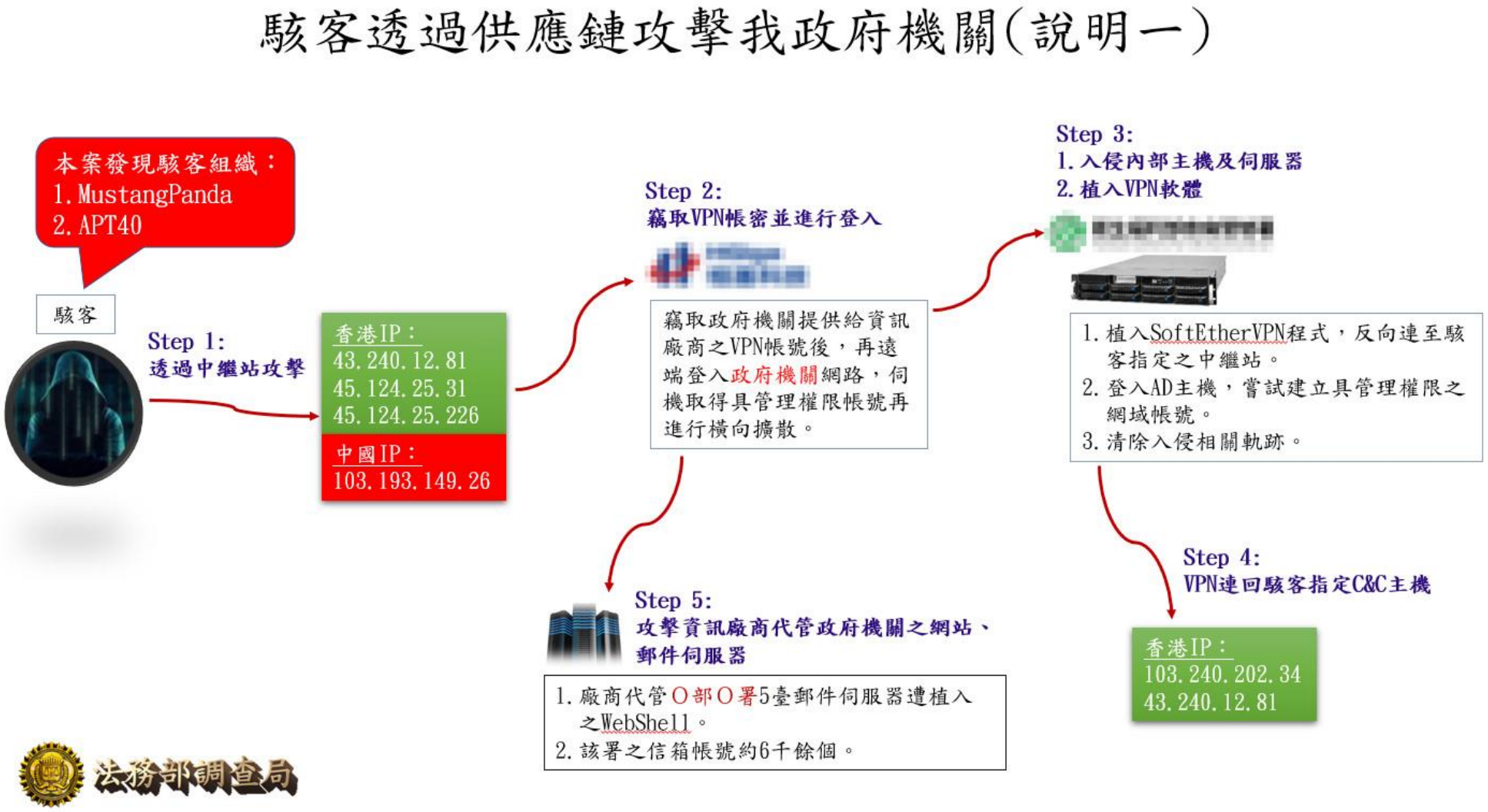
- 如何了解【關係企業/系所/社團】的資安水平?
- 是【聲譽共同】?還是【事不關己】?
- 是【捨我其誰】?還是【各自努力】?

供應鏈安全

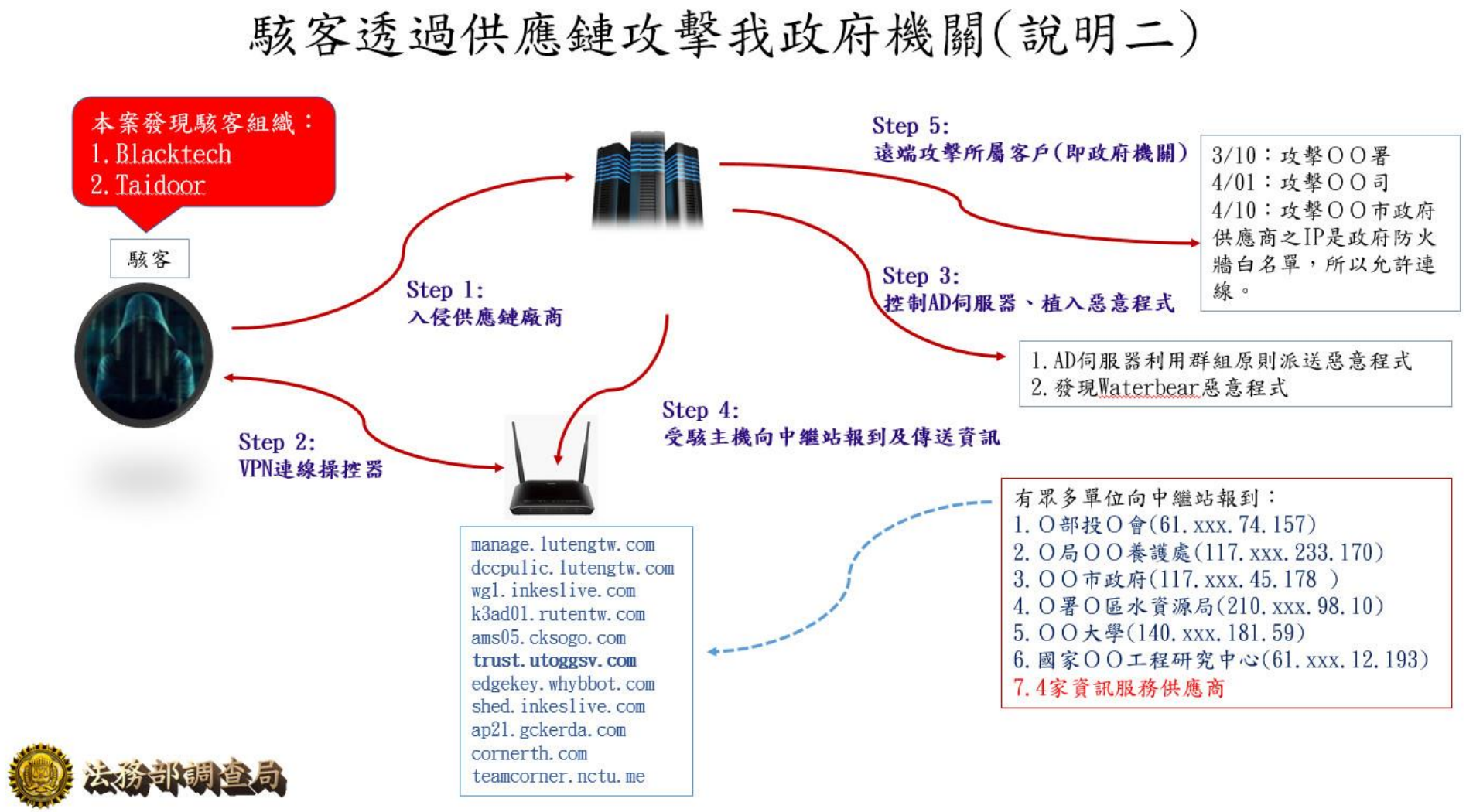
- 如何了解【策略夥伴/委外廠商】的資安水平？
- For 金融業
  - 助於評估 【Open Bank/Open API/金融科技】 的合作安全?
- For 學術單位/政府機關/高科技/電子商務
  - 助於評估【委外廠商/上下游供應鏈】的連線安全?



承包政府標案的【供應鏈廠商】成資安破口 - 1/2



承包政府標案的【供應鏈廠商】成資安破口 - 2/2



駭客透過【供應鏈攻擊】美國政府與資安公司

2020-1208 FireEye 坦承遭國家等級駭客攻擊

- 駭客成功入侵 FireEye 並且置放惡意程式在 SolarWinds 的 Orion Platform 釋出更新版本，
- 導致 FireEye 內部的 Solarwinds 軟體被駭客利用，導致 【FireEye 紅軍演練工具】外洩

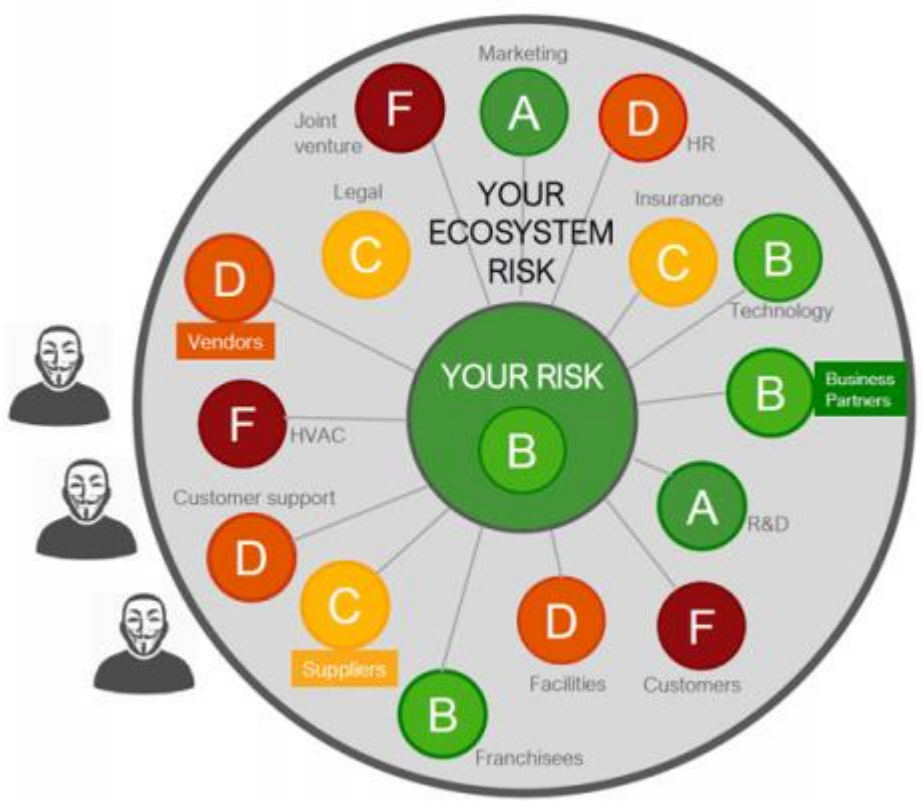
2020-1213 駭客透過【供應鏈攻擊】美國財政部與商務部

- 美國的財政部與商務部近日遭到駭客攻擊，美國國土安全部所屬的網路安全與基礎設施安全局 CISA 要求
- 所有聯邦機構【關閉】SolarWinds Orion 這款 IT 監管平臺。

2020-1214 SolarWinds 坦承駭客成功入侵其 Orion Platform 更新軟體

- 從 2020 年 3 月到 6 月間釋出的 SolarWinds Orion Platform 2019.4 HF 5 至 2020.2.1 版本
- 遭到駭客攻擊，目前安裝含漏洞 Orion Platform 版本的客戶數接近 【1.8 萬】家。

機關 63% 的資安事故-源自【生態系】資安漏洞



- 資訊安全【不再是】自己資訊處做好即可，所有系所、社團、委外資服廠商、供應鏈、合作廠商，已經構成一個【資安共同生態系】！
- 任何一個生態系的成員的資安水平都會【相互關聯與衝擊影響】！
- 駭客往往從【生態系較弱成員】下手攻擊，然後可以快速與便利地成功【擴散/蔓延/感染/牽累】到【整個生態系】！
- 所以【整體生態系風險管理】儼然成為資安防護趨勢

感謝聆聽 期待中獎

活動辦法：

凡到 CyberWin 攤位填寫問卷，即可參加【抽獎】。

獎品項目：

頭獎：Apple Airpods Pro (共抽出 1 名)
二獎：Yayusi C7 無線藍牙音箱 (共抽出 2 名)

Q & A